EMERGING NATIONAL SECURITY CONCERNS AND BUILDING STATE RESILIENCE

Date: November 22, 2022

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 22, 2022, the Honourable David McGuinty, Chairman of the National Security and Intelligence Committee of Parliamentarians (NSICOP), presented on *Emerging National Security Concerns and Building State Resilience*. The key points discussed were what is NSICOP, how NSICOP conducts reviews into Canada's National Security and Intelligence community, and the future of NSICOP's mandate. The presentation was followed by a question-and-answer period with questions from the audience and CASIS Vancouver executives.

NATURE OF DISCUSSION

Presentation

Chairman McGuinty discussed aspects of the NSICOP Act that enable NSICOP to gather information and the criteria the Committee uses for examining an issue, furthering NSCIOP's goal of providing critical review of the NSI Community and contributing to an informed public debate on NSI issues. He then summarised the findings and recommendations of seven NSICOP reviews and outlined indicators of the Committee's success, describing the current challenges NSICOP faces when conducting reviews.

Question & Answer Period

The implications of soft-violence and interdepartmental collaboration when responding to non-criminal acts of violence were discussed, with all questions answered by Executive Director for Secretariat of the NSICOP Lisa-Marie Inman on behalf of Chairman McGuinty.

BACKGROUND

Presentation

NSICOP has the mandate to review the framework, legislation, regulations, policy, administration, and finances of Canada's national security and intelligence (NSI) community. NSICOP can review any departmental activity and may review any matter related to NSI that a Minister or Prime Minister refers. The Committee is composed of a chair and 10 members from the Houses of Commons and Senate of Canada, representing all major political parties. Committee members must obtain and maintain a Top Secret clearance and swear an oath of secrecy. The membership serves as a proxy group for Parliament and Canadian society, examining NSI issues through a broad range of experiences and perspectives.

The Committee is empowered through the NSICOP Act to access any relevant information held by a government department; with the exceptions of cabinet confidences, confidential sources in witness protection programs, and information pertaining to ongoing investigations that may lead to prosecution. The Committee has a number of key objectives including: 1) publishing findings and recommendations that strengthens the NSI community in effectiveness and accountability and 2) publishing reports and reviews that inform Canadians on the activities of the NSI community.

The Committee's main accountability mechanism lies in its freedom to decide its reviews, a process which utilises five criteria: 1) whether the issue was previously reviewed; 2) how the organisation's activities are governed, its statutory authorities, and the effectiveness thereof; 3) the extent to which the activities involve the privacy and democratic rights of Canadian citizens; 4) whether there is high-level public interest and knowledge of the activities; and 5) whether Parliament or another review body has reviewed the issues. To date NSICOP has published four annual reports, four special reports, and nine substantive reviews.

In its inaugural year, the Committee reviewed how intelligence priorities are set within the NSI community, examined accountability mechanisms to manage risk, and assessed performance. The recommendations are designed to improve a process that already possesses a solid foundation.

The Committee examined the intelligence activities of the Department of National Defence (DND) and the Canadian Armed Forces (CAF), recommending that both strengthen their current accountability framework, including ongoing

independent review. The review also recommended that defence intelligence should be based on a permanent statutory footing, and these recommendations were reinforced in a subsequent special report. The Prime Minister mandated the introduction of a new framework on how CAF and DND gathers, manages, and uses defence intelligence as recommended by NSICOP.

In a subsequent review, the Committee found that government response to foreign interference was done on a case-by-case and, at times, ad hoc basis. The Committee called for a government-wide strategy to counter foreign interference and build institutional resilience, although this recommendation has not been implemented.

The Committee also conducted a review of diversity and inclusion, establishing a baseline position for the NSI community regarding certain designated groups. It was found that representation of designated groups was lower than general public service, and rates of harassment and discrimination were high within the NSI community. There is intention to follow up on progress made regarding diversity and inclusion.

The Committee provided the Prime Minister with a consolidated overview on national security threats to Canada in light of the COVID-19 pandemic. The review sought to understand if the pandemic affected threats including terrorism, the rise of Ideologically Motivated Violent Extremism (IMVE) and increased anti-government rhetoric, lockdowns disrupting terrorism facilitation, and protests. It was found that the pandemic created opportunities for foreign states to target Canada's health sector regarding vaccine development.

The Committee issued special reports on the government's framework and activities to defend its systems and networks from cyber-attacks. The government has developed a strong cyber defence system, but its framework is inconsistently applied and does not extend to all federal departments. Recommendations included bringing all federal departments under the government's cyber defence perimeter and providing them with a full range of cyber defence tools. The government agreed to all NSICOP's recommendations.

A report on the NSI activities of Global Affairs Canada (GAC) was recently tabled, finding that GAC lacks the policies, procedures, frameworks, and governance to help facilitate the work of other NSI organisations; including the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE). The Committee views that terrorist hostage-taking framework reforms should be driven by political leadership through a

government-wide approach, recommending a general policy framework to guide departmental activities and provide direction at the onset of an incident.

The Committee developed four ways to measure its success: 1) non-partisan commitment; 2) mutual trust between the Committee, the NSI community, and NSICOP Secretariat; 3) commitment to the security and safeguarding of information shared, and 4) providing informed, credible, and professional contributions to the debate of national security matters.

NSICOPs legislation requires a review after five years and will examine possible changes the Committee requires to continue its work. The chairman recently highlighted the lack of access to cabinet confidences as a challenge. NSICOP is not allowed to look into cabinet confidences but rather the government can approve the examination of specific confidences, and broad claims on information as cabinet confidences risks undermining NSICOP's mandate of assessing transparency and accountability.

The Committee issued an annual report summarising the special report information on its work over the year, and the first right to release the annual report model will likely be followed in years to come. This includes follow ups on the Committee's recommendations to date, which will be a continuing feature. Recommendations are not binding, but departments take them seriously and seek to implement them as appropriate. NSICOP is committed to following up on previous recommendations to assess impact and return to areas as needed.

Question & Answer Period

The Committee has not addressed soft violence in any of its reports. NSICOP has recently looked at similar issues through its cyber report, and how government departments work together to address non-criminal threats; i.e. soft violence. Canada is missing a formalised framework for helping government departments collaborate on addressing soft violence.

KEY POINTS OF DISCUSSION

Presentation

- NSICOP has the mandate to review the overall framework, legislation, regulations, policy, administration, and finances of Canada's NSI community.

- NSICOP can review any departmental activity and may review any matter related to NSI that a Minister or Prime Minister refers to the Committee.
- NSICOP publishes findings to strengthen the NSI community and publishes reviews to inform Canadians on the activities of the NSI community.
- NSICOP's membership is composed of parliamentarians, bringing a broad range of experiences and perspectives to examine NSI issues.
- NSICOP is committed to following up on all previous recommendations to assess impact and return to areas as needed.

Question & Answer Period

- Canada's response to non-criminal actions by threat actors—ie., soft violence—is often based on ad hoc collaboration between government departments.

This work is licensed under a Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 International License.

© (DAVID MCGUINTY, 2023)

The Journal of Intelligence, Conflict, and Warfare
Volume 5, Issue 3

SFU LIBRARY DIGITAL PUBLISH